REMARKS

1. Applicant thanks the Examiner for the Examiner's comments, which have greatly assisted Applicant in responding.

Specifically, in the Response to Arguments, The Examiner stated the Examiner "is in doubt of the meaning of 'said administrator has selected for user defined read access'". Applicant respectfully points out that this is a novel and nonobvious feature of the claimed invention, which Applicant asserts that none of the prior art of record teach, suggest, or contemplate. It is the system administrator that creates the access control command in a filter format and that selects and controls the specific user attributes listed in such command for a user, but it is the user that determines who gets read/write access to such user attributes (hence calling them user attributes, because the user controls read/write access). The claimed invention thus provides a novel and nonobvious mechanism by which both the system administrator and the user have certain control. Support can be found in the Specification on page 3, lines 10-12, hereinbelow, describing part of what the system administrator controls.

> Access control lists (ACL) are created by the System Administrators. The ACLs list the specific attributes that the user is allowed to control read or write access. This gives the Administrators full control of what information the user can give out.

And, also on page 3, lines 6-9, describing in part that which the user can control:

> The value of the read write attributes are in an LDAP Filter format which is an Internet standard (RFC 2254). The filter properties allow the user to specify not only users local to his intranet, but users across the Internet as well.

Looking at an example from the Specification, it is readily apparent that the claimed invention provides a novel and nonobvious mechanism for a system administrator to define and create a read access command with a listing of user attributes defined by the system administrator, yet, allowing a filter attribute which facilitates the user determining who has read access, as follows:

> (On page 8, line 29 through page 9, line 5)
> The invention's ACL syntax is as follows (using the example discussed earlier):

ACL: (list of n4-read attrs) (allow (read) filterattr= "whocanreadattr")
Ex: (hobbies, emergencyContact) (allow (read) filterattr= "whocanreadattr")

ACL: (list of n4-write attrs) (allow (write) filterattr= "whocanwriteattr")
Ex: (emergencyContact) (allow (write) filterattr= "whocanwriteattr")

where the values of a whocanreadattr & whocanwriteattr are:

whocanreadattr: (((ldap:///o=abc.com?(uid=sam)) (uid=Kelly))
whocanwriteattr: (uid=Kelly)

(On page 9, lines 21-22)
Using the above example, the value of "whocanwriteattr" is plugged in by the server at runtime with "(uid=Kelly)".

It should be appreciated that while thus far, the argument is for "read access", the argument is not limited to read access only, but can be applied to the write access situation and the combination of both read and write access situation.

35 U.S.C. §103(a)

2. The Examiner rejected Claims 1-27 under 35 U.S.C. §103(a) as being unpatentable over Weschler et al. (U.S. Patent No. 6,470,332), Hann et al. (U.S. Patent No. 4,799,153), and Albrecht et al. (U.S. Patent No. 5,950,011).

Applicant respectfully disagrees.

Claims 1, 10, and 19:

The Examiner stated that Weschler rendered obvious independent claims 1, 10, and 19 by the following:

"...said system administrator defined ..." and cited col. 2, lines 35-37 and col. 1, lines 55-59; as well as

"...read access control command..." at col. 8, lines 1-15, col. 8, lines 56-59, and col. 7, lines 56-59.

First, again Applicant asserts that the Examiner has broken up the description of a single feature incorrectly into parts, namely, "said administrator defined" and "read access control command". The "administrator defined" **qualifies** the "read access control command". It doesn't make sense and indeed is not fair to the prosecution of the claimed invention to assert that Weschler renders Claims 1, 10, and 19 obvlous because "system administrator defined" reads on the prior art of record, when "system administrator defined" is used as an adjective part of speech describing the "read access control command". A "system administrator defined read access control command" is one object, one entity, and cannot be broken up.

Further, on carefully reading Weschler and, in particular, col. 2, lines 35-37, Applicant again respectfully points out to the Examiner that Weschler teaches the administrator **tracking** location and content of each configuration file, which simply is not teaching a system administrator defined read access control command. Applicant is of the opinion that it is improper to deny allowability of Claims 1, 10, and 19 based on an incorrect assertion that the claimed invention (said system administrator defined) reads on Weschler at col. 2, lines 35-37. This simply is an incorrect basis for rejection.

Also, the Examiner cited col. 1, lines 55-59, which states (emphasis added by the Examiner): "... Each software application running on the client, or the client's operating system("OS") may save client specific configuration data that is used by the **client** to fine-tune and **define** the user's software environment at runtime...". Again, this is **not** teaching a "**system administrator defined** read access control command". It is unfair to deny allowability of Claims 1, 10, and 19 based on an incorrect assertion that the claimed invention (said system administrator defined) reads on Weschler at col. 2, lines 35-37. This again is simply an incorrect basis for rejection.

Regarding "...read access control command..." at col. 8, lines 1-15, col. 8, lines 56-59, and col. 7, lines 56-59, Applicant respectfully points out the following:

Col. 8, lines 1-15 cite (emphasis added by the Examiner):

> "... This metadata includes, but is not limited to, ...**read-write-modify permissions...** ." And, "The specific example of FIG. 2 includes... **lightweight directory access protocol** 207,...."

However, Weschler is just mentioning read-write-modify permissions, but is not teaching the system administrator defined read access command of the claimed invention. Weschler is just mentioning LDAP here. Nowhere does this section, nor the entirety of Weschler, teach, suggest, or contemplate a system administrator defined read access control command of the claimed invention. To use the above as a basis for rendering the claimed invention obvious is improper.

Again, the Examiner cited col. 8, lines 56-59 which read, "... Specific attributes can be requested as a return value with access control being checked." Again, Weschler is merely mentioning that specific attributes can be requested and access control is checked. This is **not teaching** the claimed invention's: system administrator defined read access control command, as fully defined in Claims 1, 10, and 19. To deny allowability of Claims 1, 10, and 19 using this as a basis for Weschler rending the claimed invention obvious is improper.

Finally, the Examiner cited col. 7, lines 56-59, which states (emphasis added by the Examiner) "...API 203 provides an interface that enables client applications that have a corresponding interface to send messages that enable the application to send data and **commands** to request profile services from core profile engine 201...". Applicant is of the opinion that this is irrelevant to the claimed invention. At best, according to the claimed invention, it is clients whose ids are listed in the user's read/write access lists (whocanreadattr and whocanwriteattr) that, during runtime, actually request to read/write such attributes of the user. So, here, the comparison made by the Examiner is not correct in that it is trying to show that Weschler teaches the system administrator define read (write) access control command. But, the command cited by Weschler is a command sent by a client application's interface to a core profile engine. Again, what Weschler is describing is irrelevant to the system administrator defined read (write) access control command of the claimed invention.

Therefore, Applicant is of the opinion that Claims 1, 10, and 19 are not rendered obvious by Weshcler in view of the discussion hereinabove. Accordingly, because not all limitations are taught, suggested, or comtemplated by Weschler. Additionally, Weschler, Hann, and

Albrecht alone or in combination do not teach, suggest, or contemplate the claimed invention, and specifically, Claims 1, 10, and 19. Accordingly, Applicant is of the opinion that Claims 1, 10, and 19 overcome the rejection under under 35 U.S.C. §103(a) and are in allowable condition. Hence, all respective dependent claims are deemed in allowable condition. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

Claims 5, 14, and 23:

The rejection of amended Claims 5, 14, and 23 and the respective dependent claims is deemed moot in view of Applicant's remarks regarding Claims 1, 10, and 19, hereinabove. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

Claims 6, 15, and 24:

The rejection of amended Claims 6, 15, and 24 and the respective dependent claims is deemed moot in view of Applicant's remarks regarding Claims 1, 10, and 19, above. Therefore, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

CONCLUSION

Based on the foregoing, Applicant considers the present invention to be distinguished from the art of record. Accordingly, Applicant earnestly solicits the Examiner's withdrawal of the rejections raised in the above referenced Final Office Action, such that a Notice of Allowance is forwarded to Applicant, and the present application is therefore allowed to issue as a United States patent.

Respectfully Submitted,

Michael A. Glenn
Reg. No. 30,176

Customer number 22862.